

1 Joseph M. Lyon (CAL Bar # 351117)

2 **THE LYON FIRM**

2754 Erie Avenue

Cincinnati, OH 45208

3 Telephone: (513) 381-2333

Facsimile: (513) 766-9011

4 Email: jlyon@thelyonfirm.com

5 *Attorney for Plaintiff and Putative Class*

6  
7  
8 **UNITED STATES DISTRICT COURT**  
9 **FOR THE CENTRAL DISTRICT OF CALIFORNIA**

10 MARK GIANNELLI, individually and  
11 on behalf of all others similarly situated,

12 Plaintiff,

13  
14 v.

15 HOUSER LLP,

16 Defendant.  
17

Case No.: 8:24-cv-00470

**CLASS ACTION COMPLAINT**

**JURY TRIAL DEMANDED**

18 **PLAINTIFF'S ORIGINAL CLASS ACTION COMPLAINT**  
19

20 Plaintiff Mark Giannelli ("Plaintiff") brings this Class Action Complaint  
21 against Houser LLP ("Defendant"), individually and on behalf of all others similarly  
22 situated ("Class Members"), and alleges, upon personal knowledge as to his own  
23 actions and his counsel's investigations, and upon information and belief as to all  
24 other matters, as follows:  
25  
26  
27  
28

1        1. Defendant is a law firm that serves Fortune 500 companies and  
2 businesses of all sizes with eleven offices nationwide.<sup>1</sup>

3  
4        2. Plaintiff brings this class action against Defendant for its failure to  
5 properly secure and safeguard personally identifiable information including, but not  
6 limited to, Plaintiff and Class Members' names, Social Security numbers, driver's  
7 license numbers, tax identification numbers, financial account information, and  
8 medical information (collectively, "Private Information").  
9

10  
11        3. To provide its legal services, Defendant stored and utilized Plaintiff's  
12 and Class Members' Private Information. By obtaining, collecting, using, and  
13 deriving a benefit from the Private Information of Plaintiff and Class Members,  
14 Defendant assumed legal and equitable duties to those individuals to protect and  
15 safeguard that information from unauthorized access and intrusion. By voluntarily  
16 undertaking the collection of this sensitive Private Information, Defendant assumed  
17 a duty to use due care to protect that information.  
18  
19

20  
21        4. Despite its duties to Plaintiff and Class Members, Defendant stored  
22 their Private Information on a database that was negligently and/or recklessly  
23 configured. This misconfiguration allowed files on the database to be accessed  
24 without a password or any form of multifactor authentication.  
25  
26

27  
28  

---

<sup>1</sup> <https://houser-law.com/> (last visited March 5, 2024).

1       5.     On May 9, 2023, Defendant discovered an unauthorized party gained  
2 access to its systems between May 7 and May 9, 2023 (the “Data Breach”).<sup>2</sup>  
3

4       6.     Plaintiff brings this class action lawsuit on behalf of those similarly  
5 situated to address Defendant’s inadequate safeguarding of Plaintiff’s and Class  
6 Members’ Private Information that it collected and maintained, and for failing to  
7 provide adequate notice to Plaintiff and other Class Members.  
8

9       7.     Defendant maintained the Private Information in a reckless and  
10 negligent manner. In particular, the Private Information was maintained on a  
11 database that was not password protected and therefore accessible to any member of  
12 the public. Foreseeably, cybercriminals exploited this obvious vulnerability,  
13 exfiltrated Plaintiff’s and Class Members’ Private Information from the database,  
14 and then listed this information for sale on the dark web.  
15  
16

17       8.     As a result of the Data Breach, Plaintiff and roughly 325,000 Class  
18 Members suffered ascertainable losses, including but not limited to, a loss of  
19 privacy, the loss of the benefit of their bargain, out-of-pocket monetary losses and  
20 expenses, the value of their time reasonably incurred to remedy or mitigate the  
21 effects of the attack, the diminished value of their Private Information, and the  
22  
23  
24  
25

---

26 <sup>2</sup> Data Breach Notifications, Office of the Maine Attorney General,  
27 [https://apps.web.maine.gov/online/aevviewer/ME/40/f0c4fd5b-bb10-48f3-82f5-](https://apps.web.maine.gov/online/aevviewer/ME/40/f0c4fd5b-bb10-48f3-82f5-d46753d726a4.shtml)  
28 [d46753d726a4.shtml](https://apps.web.maine.gov/online/aevviewer/ME/40/f0c4fd5b-bb10-48f3-82f5-d46753d726a4.shtml) (last visited March 5, 2024).

1 substantial and imminent risk of identity theft. Given the theft of information that is  
2 largely static—like Social Security numbers—this risk will remain with Plaintiff and  
3 Class Members for the rest of their lives.  
4

5 9. Upon information and belief, Plaintiff's and Class Members' Private  
6 Information remains in Defendant's possession. Plaintiff and Class Members have a  
7 continuing interest in ensuring that their information is and remains safe and should  
8 be provided injunctive and other equitable relief.  
9  
10

### 11 **PARTIES**

12 10. Plaintiff Mark Giannelli is a citizen of Maine residing in Sumner,  
13 Maine.  
14

15 11. Defendant Houser LLP is a California limited liability partnership with  
16 its principal place of business at 9970 Research Drive, Irvine, California 92618.  
17 Upon information and belief, Defendants provide legal services to clients  
18 nationwide.  
19

### 20 **JURISDICTION AND VENUE**

21  
22 12. This Court has subject matter jurisdiction over this action under the  
23 Class Action Fairness Act, 28 U.S.C. § 1332(d)(2). The amount in controversy  
24 exceeds \$5 million, exclusive of interest and costs. The number of class members  
25 exceeds 100, many of whom have different citizenship from Defendant, including  
26 Plaintiff. Thus, minimal diversity exists under 28 U.S.C. § 1332(d)(2)(A).  
27  
28



1           19. Plaintiff and Class Members relied on Defendant to keep their Private  
2 Information confidential and securely maintained, to use this information for  
3 business and health purposes only, and to make only authorized disclosure of this  
4 Private Information.  
5

6           20. Plaintiff and Class Members directly or indirectly entrusted Defendant  
7 with sensitive and confidential information, including their Private Information  
8 which includes information that is static, meaning it does not change, and can be  
9 used to commit myriad financial crimes.  
10

11           21. Plaintiff and Class Members relied on Defendant to keep their Private  
12 Information confidential and securely maintained, to use this information for  
13 business purposes only, and to make only authorized disclosures of this information.  
14 Plaintiff and Class Members demand Defendant safeguard their Private Information.  
15

16           22. Defendant had a duty to adopt reasonable measures to protect the  
17 Private Information of Plaintiff and Class Members from involuntary disclosure to  
18 third parties.  
19

20  
21  
22 ***The Data Breach***

23           23. On May 9, 2023, Defendant discovered that an unauthorized party  
24 gained access to Defendant's systems between May 7, 2023, and May 9, 2023.<sup>3</sup>  
25

26  
27  
28 

---

<sup>3</sup> *Id.*

1           24. On or around February 28, 2024, Defendant notified Plaintiff and Class  
2 Members of the Data Breach (the “Notice of Data Breach”), stating:  
3

4           **What Happened?** On May 9, 2023, Houser discovered that certain  
5 files on their computer systems had been encrypted. We immediately  
6 launched an investigation, with the assistance of third-party forensic  
7 specialists, to determine the nature and scope of the activity. Our  
8 investigation determined that there was unauthorized access to our  
9 network between May 7, 2023, and May 9, 2023, during which time  
10 certain files were copied and taken from our network. However, in June  
11 2023, the unauthorized actor informed us that they deleted copies of  
12 any stolen data and would not distribute any stolen files.

13           25. Defendant’s Notice of Data Breach admits that Plaintiff and Class  
14 Members’ Private Information was accessed, copied, and taken in the Data Breach  
15 without authorization.

16           26. Despite learning of the Data Breach on May 9, 2023, Defendant waited  
17 until February 28, 2024, before informing Plaintiff and Class Members that their  
18 Private Information was involved; a delay of almost ten months.

19           27. Because Defendant failed to properly protect safeguard Plaintiff and  
20 Class Members’ Private Information, an unauthorized third party was able to access  
21 Defendant’s database, and then accessed and exfiltrated Plaintiff and Class  
22 Members’ Private Information stored on Defendant’s database. This Private  
23 Information was then likely listed for sale on the dark web as that is the *modus*  
24 *operandi* of cybercriminals.  
25  
26  
27  
28

1           28. Upon information and belief, Defendant created the risk of the Data  
2 Breach by failing to properly configure its database, allowing it to be accessed  
3 without a password or any form of multi-factor authentication. Defendant knew or  
4 should have known this, and as such owed Plaintiff and Class members a duty of  
5 due care to protect their Private Information.  
6

7  
8 ***Plaintiff Mark Giannelli's Experience***

9           29. Plaintiff is very careful about sharing his sensitive Private Information.  
10 Plaintiff has never knowingly transmitted unencrypted sensitive Private Information  
11 over the internet or any other unsecured source. Plaintiff stores any documents  
12 containing his sensitive Private Information in a safe and secure location or destroys  
13 the documents. Moreover, Plaintiff diligently chooses unique usernames and  
14 passwords for his various online accounts.  
15

16  
17           30. Plaintiff only allowed Defendant to maintain, store, and use his Private  
18 Information because he believed that Defendant would use basic security measures  
19 to protect his Private Information, such as requiring passwords and multi-factor  
20 authentication to access databases storing his Private Information. As a result,  
21 Plaintiff's Private Information was within the possession and control of Defendant  
22 at the time of the Data Breach.  
23  
24  
25

26           31. Plaintiff received a letter from Defendant dated February 28, 2024,  
27  
28

1 informing him of the Data Breach and that his Private Information was involved.<sup>4</sup>

2 32. Plaintiff suffered injury from a loss of privacy the moment that his  
3 Private Information was accessed and exfiltrated by a third party without  
4 authorization.  
5

6 33. Plaintiff has also suffered injury in the form of damages to and  
7 diminution in the value of his Private Information.  
8

9 34. The Data Breach has also caused Plaintiff to suffer imminent and  
10 impending injury arising from the substantial risk of fraud, identity theft, and misuse  
11 resulting from his Private Information being placed in the hands of criminals.  
12

13 35. This risk from the Data Breach has caused Plaintiff to spend significant  
14 time dealing with issues related to the Data Breach, which includes time spent  
15 verifying the legitimacy of the Notice of Data Breach, and self-monitoring his  
16 accounts and credit reports to ensure no fraudulent activity has occurred.  
17  
18

19 36. Defendant acknowledges the risk posed to Plaintiff and his Private  
20 Information. Indeed, Defendant has offered a 12-month credit monitoring service to  
21 Plaintiff and Class Members.  
22

23 37. The substantial risk of imminent harm and loss of privacy have both  
24 caused Plaintiff to suffer stress, fear, and anxiety.  
25

26  
27 <sup>4</sup> Breach Notice Letter, attached as Exhibit A.  
28

1       38. Plaintiff has a continuing interest in ensuring that Plaintiff's Private  
2 Information, which, upon information and belief, remains backed up in Defendant's  
3 possession, is protected, and safeguarded from future breaches.  
4

5 ***The Data Breach was Foreseeable***

6       39. As explained by the Federal Bureau of Investigation, "[p]revention is  
7 the most effective defense against ransomware and it is critical to take precautions  
8 for protection."<sup>5</sup>  
9

10       40. Defendant's data security obligations were particularly important given  
11 the substantial increase in cyberattacks and/or data breaches in the legal industry  
12 preceding the date of the breach.  
13  
14

15       41. According to the 2017 ABA Legal Technology Survey, 22% of  
16 responding law firms were hacked or experienced data breaches in 2017,<sup>6</sup> and,  
17 according to the 2020 ABA Legal Technology Survey, 29% of responding law firms  
18  
19  
20  
21  
22

---

23 <sup>5</sup> See How to Protect Your Networks from RANSOMWARE, at 3, *available at*  
24 [https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-](https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view)  
25 [cisos.pdf/view](https://www.fbi.gov/file-repository/ransomware-prevention-and-response-for-cisos.pdf/view) (last accessed Mar. 25, 2023).

26 <sup>6</sup> David G. Ries, 2017 Security, ABA TECHREPORT 2017 (Dec. 1, 2017),  
27 [https://www.americanbar.org/groups/law\\_practice/publications/techreport/2017/se-](https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security/)  
28 [curity/](https://www.americanbar.org/groups/law_practice/publications/techreport/2017/security/).

1 reported experiencing security breaches<sup>7</sup> affecting more than 46,000 Americans.<sup>8</sup>  
2 Indeed, since 2020, “more than 750,000 Americans had personal information  
3 comprised in law firm hacks.”<sup>9</sup>  
4

5 42. In light of the ever-increasing trend of cybersecurity incidents affecting  
6 law firms, Defendant knew or should have known that its electronic records would  
7 be targeted by cybercriminals.  
8

9 43. Therefore, the increase in such attacks, and attendant risk of future  
10 attacks, was widely known to the public and to anyone in Defendant’s industry,  
11 including Defendant.  
12

13 ***Value of Private Information***  
14

15 44. The Private Information of individuals remains of high value to  
16 criminals, as evidenced by the prices they will pay through the dark web. Numerous  
17 sources cite dark web pricing for stolen identity credentials. For example, personal  
18 information can be sold at a price ranging from \$40 to \$200, and bank details have  
19  
20

---

21 <sup>7</sup> John G. Loughnane, 2020 Cybersecurity, ABA TECHREPORT (Oct. 19, 2020),  
22 [https://www.americanbar.org/groups/law\\_practice/publications/techreport/2020/cybersecurity/](https://www.americanbar.org/groups/law_practice/publications/techreport/2020/cybersecurity/).  
23

24 <sup>8</sup> Dan Roe, Cyberattacks ‘Inevitable’ for Law Firms, Highlighting Need for  
25 Comprehensive Incident Response Plans, LAW.COM (Jan. 10, 2023),  
26 <https://www.law.com/americanlawyer/2023/01/10/cyberattacks-inevitable-for-law-firms-highlighting-need-for-comprehensive-incident-response-plans/?slreturn=20230313110804>.  
27

28 <sup>9</sup> *Id.*

1 a price range of \$50 to \$200.<sup>10</sup> Experian reports that a stolen credit or debit card  
2 number can sell for \$5 to \$110 on the dark web.<sup>11</sup> Criminals can also purchase access  
3 to entire company data breaches from \$900 to \$4,500.<sup>12</sup>  
4

5 45. Based on the foregoing, the information compromised in the Data  
6 Breach is significantly more valuable than the loss of, for example, credit card  
7 information in a retailer data breach because, there, victims can cancel or close credit  
8 and debit card accounts.  
9

10 46. This data demands a much higher price on the black market. Martin  
11 Walter, senior director at cybersecurity firm RedSeal, explained, “Compared to  
12 credit card information, personally identifiable information...[is] worth more than  
13 10x on the black market.”<sup>13</sup>  
14  
15  
16  
17

---

18 <sup>10</sup> *Your personal data is for sale on the dark web. Here’s how much it costs*, Digital  
19 Trends, Oct. 16, 2019, available at:  
20 <https://www.digitaltrends.com/computing/personal-data-sold-on-the-dark-web-how-much-it-costs/> (last accessed Mar. 25, 2023).

21 <sup>11</sup> *Here’s How Much Your Personal Information Is Selling for on the Dark Web*,  
22 Experian, Dec. 6, 2017, available at: <https://www.experian.com/blogs/ask-experian/heres-how-much-your-personal-information-is-selling-for-on-the-dark-web/> (last accessed Mar. 25, 2023).

24 <sup>12</sup> *In the Dark*, VPNOverview, 2019, available at:  
25 <https://vpnoverview.com/privacy/anonymous-browsing/in-the-dark/> (last accessed Mar. 25, 2023).

26 <sup>13</sup> Time Greene, *Anthem Hack: Personal Data Stolen Sells for 10x Price of Stolen*  
27 *Credit Card Numbers*, IT World, (Feb. 6, 2015),  
28 <https://www.networkworld.com/article/2880366/anthem-hack-personal-data->

1           47. Moreover, there may be a time lag between when harm occurs versus  
2 when it is discovered, and also between when Private Information is stolen and when  
3 it is used. According to the U.S. Government Accountability Office (“GAO”), which  
4 conducted a study regarding data breaches:  
5

6           [L]aw enforcement officials told us that in some cases, stolen data may  
7 be held for up to a year or more before being used to commit identity  
8 theft. Further, once stolen data have been sold or posted on the Web,  
9 fraudulent use of that information may continue for years. As a result,  
10 studies that attempt to measure the harm resulting from data breaches  
11 cannot necessarily rule out all future harm.<sup>14</sup>

12           48. At all relevant times, Defendant knew, or reasonably should have  
13 known, of the importance of safeguarding the Private Information of Plaintiff and  
14 Class Members and the foreseeable consequences that would occur if Defendant’s  
15 data security system was breached, including, specifically, the significant costs that  
16 would be imposed on Plaintiff and Class Members as a result of a breach.  
17

18           49. Plaintiff and Class Members now face years of constant surveillance of  
19 their financial and personal records, monitoring, and loss of rights. The Class is  
20 incurring and will continue to incur such damages in addition to any fraudulent use  
21 of their Private Information.  
22

23  
24  
25 stolen-sells-for-10x-price-of-stolen-credit-card-numbers.html (last accessed Mar.  
26 25, 2023).

27 <sup>14</sup> *Report to Congressional Requesters*, GAO, at 29 (June 2007),  
28 <https://www.gao.gov/assets/gao-07-737.pdf> (last accessed Aug. 23, 2021).

1           50. Defendant was, or should have been, fully aware of the unique type and  
2 the significant volume of data on Defendant's network and, thus, the significant  
3 number of individuals who would be harmed by the exposure of the unencrypted  
4 data.  
5

6           51. The injuries to Plaintiff and Class Members were directly and  
7 proximately caused by Defendant's failure to implement or maintain adequate data  
8 security measures for the Private Information of Plaintiff and Class Members.  
9

10           52. By obtaining, collecting, using, and deriving a benefit from Plaintiff's  
11 and Class Members' Private Information, Defendant assumed legal and equitable  
12 duties and knew or should have known that it was responsible for protecting  
13 Plaintiff's and Class Members' Private Information from unauthorized disclosure.  
14

15           53. Plaintiff and the Class Members have taken reasonable steps to  
16 maintain the confidentiality of their Private Information.  
17

18           54. Plaintiff and the Class Members relied on Defendant to implement and  
19 follow adequate data security policies and protocols, to keep their Private  
20 Information confidential and securely maintained, to use such Private Information  
21 solely for business and health care purposes, and to prevent the unauthorized  
22 disclosures of the Private Information.  
23  
24  
25

26 ***Defendant Failed to Properly Protect Plaintiff's and Class Members' Private***  
27 ***Information***  
28

1  
2 55. Defendant could have prevented this Data Breach by properly securing  
3 and encrypting the systems containing the Private Information of Plaintiff and Class  
4 Members. Alternatively, Defendant could have destroyed the data, especially for  
5 individuals with whom it had not had a relationship for a period of time.  
6

7  
8 56. Defendant's negligence in safeguarding the Private Information of  
9 Plaintiff and Class Members is exacerbated by the repeated warnings and alerts  
10 directed to companies like Defendant to protect and secure sensitive data they  
11 possess.  
12

13 57. Despite the prevalence of public announcements of data breach and  
14 data security compromises, Defendant failed to take appropriate steps to protect the  
15 Private Information of Plaintiff and Class Members from being compromised.  
16

17 58. To prevent and detect unauthorized cyber-attacks, Defendant could and  
18 should have implemented, as recommended by the United States Government, the  
19 following measures:  
20

- 21 • Implement an awareness and training program. Because end  
22 users are targets, employees and individuals should be aware of  
23 the threat of ransomware and how it is delivered.
- 24 • Configure firewalls to block access to known malicious IP  
25 addresses.
- 26 • Patch operating systems, software, and firmware on devices.  
27 Consider using a centralized patch management system.  
28

- Manage the use of privileged accounts based on the principle of least privilege: no users should be assigned administrative access unless absolutely needed; and those with a need for administrator accounts should only use them when necessary.
- Configure access controls—including file, directory, and network share permissions—with least privilege in mind. If a user only needs to read specific files, the user should not have write access to those files, directories, or shares.
- Disable macro scripts from office files transmitted via email. Consider using Office Viewer software to open Microsoft Office files transmitted via email instead of full office suite applications.
- Implement Software Restriction Policies (SRP) or other controls to prevent programs from executing from common ransomware locations, such as temporary folders supporting popular Internet browsers or compression/decompression programs, including the AppData/LocalAppData folder.
- Consider disabling Remote Desktop protocol (RDP) if it is not being used.
- Use application whitelisting, which only allows systems to execute programs known and permitted by security policy.
- Execute operating system environments or specific programs in a virtualized environment
- Categorize data based on organizational value and implement physical and logical separation of networks and data for different organizational units.<sup>15</sup>

59. To prevent and detect cyber-attacks, including the cyber-attack that resulted in the Data Breach, Defendant could and should have implemented, as

---

<sup>15</sup> *Id.* at 3-4.

recommended by the Microsoft Threat Protection Intelligence Team, the following measures:

**Secure internet-facing assets**

- Apply latest security updates
- Use threat and vulnerability management
- Perform regular audit; remove privileged credentials;

**Include IT Pros in security discussions**

- Ensure collaboration among [security operations], [security admins], and [information technology] admins to configure servers and other endpoints securely;

**Build credential hygiene**

- Use [multifactor authentication] or [network level authentication] and use strong, randomized, just-in-time local admin passwords

**Apply principle of least-privilege**

- Monitor for adversarial activities
- Hunt for brute force attempts
- Monitor for cleanup of Event Logs
- Analyze logon events

60. Given that Defendant was storing the Private Information of Plaintiff and Class Members, Defendant could and should have implemented all of the above measures to prevent and detect cyberattacks. Instead, Defendant failed to implement

1 basic security measures, like password protection, encryption, or multifactor  
2 authentication.

3  
4 ***Defendant Failed to Comply with FTC Guidelines***

5         61. The Federal Trade Commission (“FTC”) has promulgated numerous  
6 guides for businesses which highlight the importance of implementing reasonable  
7 data security practices. According to the FTC, the need for data security should be  
8 factored into all business decision making.  
9

10  
11         62. In 2016, the FTC updated its publication, Protecting Personal  
12 Information: A Guide for Business, which established cyber-security guidelines for  
13 businesses. The guidelines note that businesses should protect the personal patient  
14 information that they keep; properly dispose of personal information that is no longer  
15 needed; encrypt information stored on computer networks; understand their  
16 network’s vulnerabilities; and implement policies to correct any security problems.<sup>16</sup>  
17

18  
19         63. The FTC further recommends that companies not maintain Private  
20 Information longer than is needed for authorization of a transaction; limit access to  
21 sensitive data; require complex passwords to be used on networks; use industry-  
22

23  
24  
25 <sup>16</sup> Protecting Personal Information: A Guide for Business, Federal Trade  
26 Commission (2016). [https://www.ftc.gov/system/files/documents/plain-](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf)  
27 [language/pdf-0136\\_proteting-personal-information.pdf](https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf).  
28

1 tested methods for security; monitor for suspicious activity on the network; and  
2 verify that third-party service providers have implemented reasonable security  
3 measures.  
4

5         64. The FTC has brought enforcement actions against businesses for failing  
6 to adequately and reasonably protect patient data, treating the failure to employ  
7 reasonable and appropriate measures to protect against unauthorized access to  
8 confidential consumer data as an unfair act or practice prohibited by Section 5 of the  
9 Federal Trade Commission Act (“FTCA”), 15 U.S.C. § 45. Orders resulting from  
10 these actions clarify the measures businesses take to meet their data security  
11 obligations.  
12  
13  
14

15         65. Defendant failed to properly implement basic data security practices,  
16 such as making a database storing Private Information available to the public without  
17 the use of a password or multifactor authentication.  
18

19         66. Defendant’s failure to employ reasonable and appropriate measures to  
20 protect against unauthorized access to Plaintiff’s and Class Members’ Private  
21 Information constitutes an unfair act or practice prohibited by Section 5 of the FTC  
22 Act, 15 U.S.C. § 45.  
23  
24

25         67. Defendant was always fully aware of its obligation to protect the Private  
26 Information of Plaintiff and Class members. Defendant was also aware of the  
27 significant repercussions that would result from its failure to do so.  
28

***Defendant failed to Comply with Industry Standards***

68. Several best practices have been identified that at a minimum should be implemented by service providers like Defendant, including but not limited to: educating all employees; strong passwords; multi-layer security, including firewalls, anti-virus, and antimalware software; encryption, making data unreadable without a key; multi-factor authentication; backup data; and limiting which employees can access sensitive data.

69. Defendant failed to meet the minimum standards of any of the following frameworks: the NIST Cybersecurity Framework Version 1.1 (including without limitation PR.AC-1, PR.AC-3, PR.AC-4, PR.AC-5, PR.AC-6, PR.AC-7, PR.AT-1, PR.DS-1, PR.DS-5, PR.PT-1, PR.PT-3, DE.CM-1, DE.CM-4, DE.CM-7, DE.CM-8, and RS.CO-2), and the Center for Internet Security's Critical Security Controls (CIS CSC), which are all established standards in reasonable cybersecurity readiness.

70. The foregoing frameworks are existing and applicable industry standards in the legal industry, and Defendant failed to comply with these accepted standards, thereby opening the door to and causing the Data Breach.

***As a Result of Defendant's Failure to Safeguard Private Information, Plaintiff and the Proposed Class Face Significant Risk of Continued Identity Theft and Have Experienced Substantial Harm***

71. Plaintiff and members of the proposed Class have suffered injury from

1 the access to, and misuse of, their Private Information that can be directly traced to  
2 Defendant.

3  
4 72. The ramifications of Defendant's failure to keep Plaintiff's and the  
5 Class's Private Information secure are severe. Identity theft occurs when someone  
6 uses another's personal and financial information such as that person's name,  
7  
8 account number, Social Security number, driver's license number, date of birth,  
9  
10 and/or other information, without permission, to commit fraud or other crimes.

11 73. The FTC defines identity theft as "a fraud committed or attempted using  
12 the identifying information of another person without authority." The FTC describes  
13 "identifying information" as "any name or number that may be used, alone or in  
14  
15 conjunction with any other information, to identify a specific person," including,  
16  
17 among other things, "[n]ame, Social Security number, date of birth, official State or  
18  
19 government issued driver's license or identification number, alien registration  
20  
21 number, government passport number, employer or taxpayer identification number."

22 74. According to experts, one out of four data breach notification recipients  
23  
24 become a victim of identity fraud.

25 75. As a result of Defendant's failures to prevent—and to timely detect—  
26  
27 the Data Breach, Plaintiff and the proposed Class have suffered and will continue to  
28  
suffer damages, including monetary losses, lost time, anxiety, and emotional  
distress. They have suffered or are at an increased risk of suffering:

- a. The loss of the opportunity to control how their Private Information is used;
- b. The diminution in value of their Private Information;
- c. The compromise and continuing publication of their Private Information;
- d. Out-of-pocket costs associated with the prevention, detection, recovery, and remediation from identity theft or fraud;
- e. Lost opportunity costs and lost wages associated with the time and effort expended addressing and attempting to mitigate the actual and future consequences of the Data Breach, including, but not limited to, efforts spent researching how to prevent, detect, contest, and recover from identity theft and fraud;
- f. Delay in receipt of tax refund monies;
- g. Unauthorized use of stolen Private Information; and
- h. The continued risk to their Private Information, which remains in the possession of Defendant and is subject to further breaches so long as Defendant fails to undertake the appropriate measures to protect the Private Information in their possession.

76. One such example of criminals using Private Information for profit, to the detriment of Plaintiff and the Class Members, is the development of “Fullz” packages.

77. Cyber-criminals can cross-reference two sources of Private Information to marry unregulated data available elsewhere to criminally stolen data with an astonishingly complete scope and degree of accuracy in order to assemble complete

1 dossiers on individuals. These dossiers are known as “Fullz” packages.

2       78. The development of “Fullz” packages means that stolen Private  
3 Information from the Data Breach can easily be used to link and identify it to  
4 Plaintiff’s and the proposed Class’s phone numbers, email addresses, and other  
5 unregulated sources and identifiers. In other words, even if certain information such  
6 as emails, phone numbers, or credit card numbers may not be included in the Private  
7 Information stolen by the cyber-criminals in the Data Breach, criminals can easily  
8 create a Fullz package and sell it at a higher price to unscrupulous operators and  
9 criminals (such as illegal and scam telemarketers) over and over. That is exactly  
10 what is happening to Plaintiff and members of the proposed Class, and it is  
11 reasonable for any trier of fact, including this Court or a jury, to find that Plaintiff’s  
12 and other members of the proposed Class’s stolen Private Information is being  
13 misused, and that such misuse is fairly traceable to the Data Breach.

14       79. According to the FBI’s Internet Crime Complaint Center (IC3) 2019  
15 Internet Crime Report, Internet-enabled crimes reached their highest number of  
16 complaints and dollar losses that year, resulting in more than \$3.5 billion in losses  
17 to individuals and business victims.

18       80. Further, according to the same report, “rapid reporting can help law  
19 enforcement stop fraudulent transactions before a victim loses the money for good.”  
20 Defendant did not rapidly report to Plaintiff and the Class that their Private  
21

1 Information had been stolen, and in fact did not notify Plaintiff for five months.

2 81. Victims of identity theft also often suffer embarrassment, blackmail, or  
3 harassment in person or online, and/or experience financial losses resulting from  
4 fraudulently opened accounts or misuse of existing accounts.  
5

6 82. In addition to out-of-pocket expenses that can exceed thousands of  
7 dollars and the emotional toll identity theft can take, some victims have to spend a  
8 considerable time repairing the damage caused by the theft of their Private  
9 Information. Victims of new account identity theft will likely have to spend time  
10 correcting fraudulent information in their credit reports and continuously monitor  
11 their reports for future inaccuracies, close existing bank/credit accounts, open new  
12 ones, and dispute charges with creditors.  
13  
14  
15

16 83. Further complicating the issues faced by victims of identity theft, data  
17 thieves may wait years before attempting to use the stolen Private Information. To  
18 protect themselves, Plaintiff and the Class will need to remain vigilant against  
19 unauthorized data use for years or even decades to come.  
20  
21

22 84. According to the FTC, unauthorized Private Information disclosures  
23 are extremely damaging to consumers' finances, credit history and reputation, and  
24  
25  
26  
27  
28

1 can take time, money and patience to resolve the fallout.<sup>17</sup> The FTC treats the failure  
2 to employ reasonable and appropriate measures to protect against unauthorized  
3 access to confidential consumer data as an unfair act or practice prohibited by  
4 Section 5(a) of the FTC Act.  
5

6 85. Defendant's failure to properly notify Plaintiff and Class Members of  
7 the Data Breach exacerbated Plaintiff and Class Members' injury by depriving them  
8 of the earliest ability to take appropriate measures to protect their Private  
9 Information and take other necessary steps to mitigate the harm caused by the Data  
10 Breach.  
11

12  
13 ***Plaintiff and Class Members' Damages***  
14

15 86. To date, Defendant has done little to provide Plaintiff and Class  
16 Members with relief for the damages they have suffered as a result of the Data  
17 Breach, including, but not limited to, the costs and loss of time they incurred because  
18 of the Data Breach. Defendant has only offered 12 months of inadequate identity  
19 monitoring services to some, but not all Class Members, despite Plaintiff and Class  
20 Members being at risk of identity theft and fraud for the remainder of their lifetimes.  
21

22 87. The 12 months of credit monitoring offered to persons whose Private  
23  
24  
25

---

26 <sup>17</sup> See Taking Charge, What to Do If Your Identity is Stolen, FTC, at 3 (2012),  
27 <https://www.ojp.gov/ncjrs/virtual-library/abstracts/taking-charge-what-do-if-your-identity-stolen> (last visited October 10, 2022).  
28

1 Information was compromised is wholly inadequate as it fails to provide for the fact  
2 that victims of data breaches and other unauthorized disclosures commonly face  
3 multiple years of ongoing identity theft and financial fraud. What's more, Defendant  
4 waited almost ten months to inform Plaintiff and Class Members that their Private  
5 Information was at risk.  
6

7  
8 88. Plaintiff and Class Members have been damaged by the compromise of  
9 their Private Information in the Data Breach.  
10

11 89. As a direct and proximate result of Defendant's conduct, Plaintiff and  
12 Class Members have been placed at an imminent, immediate, continuing, and  
13 substantial risk of harm from fraud and identity theft.  
14

15 90. Plaintiff and Class Members face substantial risk of out-of-pocket fraud  
16 losses such as loans opened in their names, medical services billed in their names,  
17 tax return fraud, utility bills opened in their names, credit card fraud, and similar  
18 identity theft.  
19

20 91. Plaintiff and Class Members face substantial risk of being targeted for  
21 future phishing, data intrusion, and other illegal schemes based on their Private  
22 Information as potential fraudsters could use that information to more effectively  
23 target such schemes to Plaintiff and Class Members.  
24

25 92. Plaintiff and Class Members may also incur out-of-pocket costs for  
26 protective measures such as credit monitoring fees, credit report fees, credit freeze  
27  
28

1 fees, and similar costs directly or indirectly related to the Data Breach.

2 93. Defendant's delay in noticing affected persons of the theft of their  
3 Private Information prevented early mitigation efforts and compounded the harm.  
4

5 94. Plaintiff and Class Members have suffered or will suffer actual injury  
6 as a direct result of the Data Breach. Many victims suffered ascertainable losses in  
7 the form of out-of-pocket expenses and the value of their time reasonably incurred  
8 to remedy or mitigate the effects of the Data Breach relating to:  
9

- 10 a. Reviewing and monitoring financial and other sensitive accounts and  
11 finding fraudulent insurance claims, loans, and/or government benefits  
12 claims;
- 13 b. Purchasing credit monitoring and identity theft prevention;
- 14 c. Placing "freezes" and "alerts" with reporting agencies;
- 15 d. Spending time on the phone with or at financial institutions, healthcare  
16 providers, and/or government agencies to dispute unauthorized and  
17 fraudulent activity in their name;
- 18 e. Contacting financial institutions and closing or modifying financial  
19 accounts; and
- 20 f. Closely reviewing and monitoring Social Security number, bank  
21 accounts, and credit reports for unauthorized activity for years to come.  
22

23 95. Moreover, Plaintiff and Class Members have an interest in ensuring that  
24 their Personal and Medical Information, which is believed to remain in the  
25 possession of Defendant, is protected from further breaches by the implementation  
26  
27  
28

1 of security measures and safeguards, including but not limited to, making sure that  
2 the storage of data or documents containing Private Information is not accessible  
3 online and that access to such data is encrypted and password protected.  
4

5 96. Defendant acknowledges the harm caused to Plaintiff and Class  
6 Members because it offered a complimentary 12-month credit monitoring program  
7 via IDX to Class Members.  
8

9 **CLASS ALLEGATIONS**  
10

11 97. Plaintiff brings this nationwide class action on behalf of himself and on  
12 behalf of others similarly situated pursuant to Rule 23(b)(2), 23(b)(3), and 23(c)(4)  
13 of the Federal Rules of Civil Procedure.  
14

15 98. The Nationwide Class that Plaintiff seek to represent is defined as  
16 follows:  
17

18 All persons whose Private Information was actually or potentially  
19 accessed or acquired during the Data Breach event that is the subject of  
20 the Notice of Data Breach that Defendant published to Plaintiff and  
21 other Class Members on or around February 28, 2024 (the “Class”).

22 99. Excluded from the Class are the following individuals and/or entities:  
23 Defendant and Defendant’s parents, subsidiaries, affiliates, officers and directors,  
24 and any entity in which Defendant has a controlling interest; all individuals who  
25 make a timely election to be excluded from this proceeding using the correct protocol  
26 for opting out; any and all federal, state or local governments, including but not  
27  
28

1 limited to their departments, agencies, divisions, bureaus, boards, sections, groups,  
2 counsels and/or subdivisions; and all judges assigned to hear any aspect of this  
3 litigation, as well as their immediate family members.  
4

5 100. Plaintiff reserves the right to modify or amend the definition of the  
6 proposed classes before the Court determines whether certification is appropriate.  
7

8 101. Numerosity, Fed R. Civ. P. 23(a)(1): Class Members are so numerous  
9 that joinder of all members is impracticable. Upon information and belief, there are  
10 certainly tens of thousands, and possibly in excess of 325,000 individuals whose  
11 Private Information was improperly accessed in the Data Breach, and each Class is  
12 apparently identifiable within Defendant's records.  
13  
14

15 102. Commonality, Fed. R. Civ. P. 23(a)(2) and (b)(3): Questions of law and  
16 fact common to the Classes exist and predominate over any questions affecting only  
17 individual Class Members. These include:  
18

- 19 a. Whether and to what extent Defendant had a duty to protect the Private  
20 Information of Plaintiff and Class Members;
- 21 b. Whether Defendant had duties not to disclose the Private Information of  
22 Plaintiff and Class Members to unauthorized third parties;
- 23 c. Whether Defendant failed to adequately safeguard the Private  
24 Information of Plaintiff and Class Members;
- 25 d. Whether and when Defendant actually learned of the Data Breach;
- 26 e. Whether Defendant adequately, promptly, and accurately informed  
27 Plaintiff and Class Members that their Private Information had been  
28

1           compromised;

2           f. Whether Defendant violated the law by failing to promptly notify  
3           Plaintiff and Class Members that their Private Information had been  
4           compromised;

5           g. Whether Defendant failed to implement and maintain reasonable security  
6           procedures and practices appropriate to the nature and scope of the  
7           information compromised in the Data Breach;

8           h. Whether Defendant adequately addressed and fixed the vulnerabilities  
9           which permitted the Data Breach to occur;

10          i. Whether Plaintiff and Class Members are entitled to actual,  
11          consequential, and/or nominal damages as a result of Defendant's  
12          wrongful conduct;

13          j. Whether Plaintiff and Class Members are entitled to restitution as a result  
14          of Defendant's wrongful conduct; and

15          k. Whether Plaintiff and Class Members are entitled to injunctive relief to  
16          redress the imminent and currently ongoing harm faced as a result of the  
17          Data Breach.

18          103. Typicality, Fed. R. Civ. P. 23(a)(3): Plaintiff's claims are typical of  
19          those of other Class Members because all had their Private Information  
20          compromised as a result of the Data Breach, due to Defendant's misfeasance.

21          104. Policies Generally Applicable to the Class: This class action is also  
22          appropriate for certification because Defendant has acted or refused to act on  
23          grounds generally applicable to the Class, thereby requiring the Court's imposition  
24          of uniform relief to ensure compatible standards of conduct toward the Class  
25          of uniform relief to ensure compatible standards of conduct toward the Class  
26          of uniform relief to ensure compatible standards of conduct toward the Class  
27          of uniform relief to ensure compatible standards of conduct toward the Class  
28

1 Members and making final injunctive relief appropriate with respect to the Class as  
2 a whole. Defendant's policies challenged herein apply to and affect Class Members  
3 uniformly and Plaintiff's challenge of these policies hinges on Defendant's conduct  
4 with respect to the Class as a whole, not on facts or law applicable only to Plaintiff.  
5

6 105. Adequacy, Fed. R. Civ. P. 23(a)(4): Plaintiff will fairly and adequately  
7 represent and protect the interests of the Class Members in that Plaintiff has no  
8 disabling conflicts of interest that would be antagonistic to those of the other  
9 Members of the Class. Plaintiff seeks no relief that is antagonistic or adverse to the  
10 Members of the Class and the infringement of the rights and the damages Plaintiff  
11 has suffered are typical of other Class Members. Plaintiff has also retained counsel  
12 experienced in complex class action litigation, and Plaintiff intends to prosecute this  
13 action vigorously.  
14

15 106. Superiority and Manageability, Fed. R. Civ. P. 23(b)(3): Class litigation  
16 is an appropriate method for fair and efficient adjudication of the claims involved.  
17 Class action treatment is superior to all other available methods for the fair and  
18 efficient adjudication of the controversy alleged herein; it will permit a large number  
19 of Class Members to prosecute their common claims in a single forum  
20 simultaneously, efficiently, and without the unnecessary duplication of evidence,  
21 effort, and expense that hundreds of individual actions would require. Class action  
22 treatment will permit the adjudication of relatively modest claims by certain Class  
23  
24  
25  
26  
27  
28

1 Members, who could not individually afford to litigate a complex claim against large  
2 corporations, like Defendant. Further, even for those Class Members who could  
3 afford to litigate such a claim, it would still be economically impractical and impose  
4 a burden on the courts.  
5

6 107. The nature of this action and the nature of laws available to Plaintiff  
7 and Class Members make the use of the class action device a particularly efficient  
8 and appropriate procedure to afford relief to Plaintiff and Class Members for the  
9 wrongs alleged because Defendant would necessarily gain an unconscionable  
10 advantage since they would be able to exploit and overwhelm the limited resources  
11 of each individual Class Member with superior financial and legal resources; the  
12 costs of individual suits could unreasonably consume the amounts that would be  
13 recovered; proof of a common course of conduct to which Plaintiff were exposed is  
14 representative of that experienced by the Class and will establish the right of each  
15 Class Member to recover on the cause of action alleged; and individual actions  
16 would create a risk of inconsistent results and would be unnecessary and duplicative  
17 of this litigation.  
18

19 108. The litigation of the claims brought herein is manageable. Defendant's  
20 uniform conduct, the consistent provisions of the relevant laws, and the ascertainable  
21 identities of Class Members demonstrates that there would be no significant  
22 manageability problems with prosecuting this lawsuit as a class action.  
23  
24  
25  
26  
27  
28

1           109. Adequate notice can be given to Class Members directly using  
2 information maintained in Defendant's records.

3  
4           110. Unless a Class-wide injunction is issued, Defendant may continue in  
5 their failure to properly secure the Private Information of Class Members, Defendant  
6 may continue to refuse to provide proper notification to Class Members regarding  
7 the Data Breach, and Defendant may continue to act unlawfully as set forth in this  
8 Complaint.  
9

10  
11           111. Further, Defendant has acted or refused to act on grounds generally  
12 applicable to the Classes and, accordingly, final injunctive or corresponding  
13 declaratory relief with regard to the Class Members as a whole is appropriate under  
14 Rule 23(b)(2) of the Federal Rules of Civil Procedure.  
15

16           112. Likewise, particular issues under Rule 23(c)(4) are appropriate for  
17 certification because such claims present only particular, common issues, the  
18 resolution of which would advance the disposition of this matter and the parties'  
19 interests therein. Such particular issues include, but are not limited to:  
20  
21

- 22           a. Whether Defendant owed a legal duty to Plaintiff and Class Members  
23           to exercise due care in collecting, storing, using, and safeguarding their  
24           Private Information;
- 25           b. Whether Defendant breached a legal duty to Plaintiff and Class  
26           Members to exercise due care in collecting, storing, using, and  
27           safeguarding their Private Information;
- 28           c. Whether Defendant failed to comply with its own policies and

1 applicable laws, regulations, and industry standards relating to data  
2 security;

3 d. Whether Defendant adequately and accurately informed Plaintiff and  
4 Class Members that their Private Information had been compromised;

5 e. Whether Defendant failed to implement and maintain reasonable  
6 security procedures and practices appropriate to the nature and scope of  
7 the information compromised in the Data Breach;

8 f. Whether Class Members are entitled to actual, consequential, and/or  
9 nominal damages, and/or injunctive relief as a result of Defendant's  
10 wrongful conduct.

## 11 **CAUSES OF ACTION**

### 12 **COUNT I** 13 **NEGLIGENCE**

14 **(On Behalf of Plaintiff and the Putative Nationwide Rule 23 Class)**

15 113. Plaintiff and the Class repeat and re-allege each and every allegation in  
16 the Complaint as if fully set forth herein.

17 114. Plaintiff and the Class entrusted Defendant with their Private  
18 Information.  
19

20 115. Plaintiff and the Class entrusted their Private Information to Defendant  
21 on the premise and with the understanding that Defendant would safeguard their  
22 information, use their information for business purposes only, and/or not disclose  
23 their Private Information to unauthorized third parties.  
24

25 116. Defendant has full knowledge of the sensitivity of the Private  
26 Information and the types of harm that Plaintiff and the Class could and would suffer  
27  
28

1 if the Private Information were wrongfully disclosed.

2 117. Defendant knew or reasonably should have known that the failure to  
3 exercise due care in the collecting, storing, and using of the Private Information of  
4 Plaintiff and the Class involved an unreasonable risk of harm to Plaintiff and the  
5 Class, even if the harm occurred through the criminal acts of a third party.  
6

7 118. By accepting, storing, and maintaining Plaintiff's and Class Members'  
8 Private Information, Defendant undertook a duty to exercise reasonable care in  
9 safeguarding, securing, and protecting such information from being compromised,  
10 lost, stolen, misused, and/or disclosed to unauthorized parties. This duty includes,  
11 among other things, designing, maintaining, and testing Defendant's security  
12 protocols to ensure that the Private Information of Plaintiff and the Class Members  
13 in Defendant's possession was adequately secured and protected.  
14

15 119. By accepting, storing, and maintaining Plaintiff's and Class Members'  
16 Private Information, Defendant also had a duty to exercise appropriate clearinghouse  
17 practices to remove Private Information they were no longer required to retain  
18 pursuant to regulations.  
19

20 120. By accepting, storing, and maintaining Plaintiff's and Class Members'  
21 Private Information, Defendant also had a duty to have procedures in place to detect  
22 and prevent the improper access and misuse of the Private Information of Plaintiff  
23 and the Class.  
24  
25  
26  
27  
28

1           121. Defendant's duty to use reasonable security measures arose as a result  
2 of the special relationship that existed between Defendant and Plaintiff and the  
3 Class. That special relationship arose because Plaintiff and the Class entrusted  
4 Defendant with their confidential Private Information, a necessary part of obtaining  
5 services from Defendant.  
6

7  
8           122. A breach of security, unauthorized access, and resulting injury to  
9 Plaintiff and the Class was reasonably foreseeable, particularly in light of  
10 Defendant's inadequate security practices.  
11

12           123. Plaintiff and the Class were the foreseeable and probable victims of any  
13 inadequate security practices and procedures. Defendant knew or should have  
14 known of the inherent risks in collecting and storing the Private Information of  
15 Plaintiff and the Class, the critical importance of providing adequate security of that  
16 Private Information, and the necessity for encrypting Private Information stored on  
17 Defendant's systems.  
18

19  
20           124. Defendant's own conduct created a foreseeable risk of harm to Plaintiff  
21 and the Class. Defendant's misconduct included, but was not limited to, their failure  
22 to take the steps and opportunities to prevent the Data Breach as set forth herein.  
23 Defendant's misconduct also included their decisions not to comply with industry  
24 standards for the safekeeping of the Private Information of Plaintiff and the Class,  
25 including basic encryption techniques freely available to Defendant.  
26  
27  
28

1           125. Defendant knew or should have known that Plaintiff's and Class  
2 Members' Private Information was stored on its database and was or should have  
3 been aware of the extreme risks associated with failing to properly safeguard  
4 Plaintiff's and Class Members' Private Information.  
5

6           126. Despite being aware of the likelihood that Defendant's databases were  
7 vulnerable, not secure, and likely to be attacked by cybercriminals, Defendant failed  
8 to correct, update, or upgrade its security protections, thus causing the Data Breach.  
9  
10

11           127. Plaintiff and the Class had no ability to protect their Private Information  
12 that was in, and possibly remains in, Defendant's possession.  
13

14           128. Defendant was in the best position to protect against the harm suffered  
15 by Plaintiff and the Class as a result of the Data Breach.  
16

17           129. Defendant had and continues to have a duty to adequately disclose that  
18 the Private Information of Plaintiff and the Class within Defendant's possession  
19 might have been compromised, how it was compromised, and precisely the types of  
20 data that were compromised and when. Such notice was necessary to allow Plaintiff  
21 and the Class to take steps to prevent, mitigate, and repair any identity theft and the  
22 fraudulent use of their Private Info by third parties.  
23

24           130. Defendant had a duty to employ proper procedures to prevent the  
25 unauthorized dissemination of the Private Information of Plaintiff and the Class.  
26

27           131. Defendant has admitted that the Private Information of Plaintiff and  
28

1 Class Members was improperly accessed, exfiltrated, and encrypted by unauthorized  
2 third persons as a result of the Data Breach.

3  
4 132. Defendant improperly and inadequately safeguarded the Private  
5 Information of Plaintiff and the Class in deviation of standard industry rules,  
6 regulations, and practices at the time of the Data Breach.  
7

8 133. Defendant, through its actions and/or omissions, unlawfully breached  
9 its duties to Plaintiff and the Class by failing to implement industry protocols and  
10 exercise reasonable care in protecting and safeguarding the Private Information of  
11 Plaintiff and the Class during the time the Private Information was within  
12 Defendant's possession or control.  
13  
14

15 134. Defendant failed to heed industry warnings and alerts to provide  
16 adequate safeguards to protect the Private Information of Plaintiff and the Class in  
17 the face of increased risk of theft.  
18

19 135. Defendant, through its actions and/or omissions, unlawfully breached  
20 its duty to Plaintiff and the Class by failing to have appropriate procedures in place  
21 to detect and prevent dissemination of Private Information.  
22

23 136. Defendant breached its duty to exercise appropriate clearinghouse  
24 practices by failing to remove Private Information they were no longer required to  
25 retain pursuant to regulations.  
26

27 137. Defendant, through its actions and/or omissions, unlawfully breached  
28

1 its duty to adequately and timely disclose to Plaintiff and the Class the existence and  
2 scope of the Data Breach.

3  
4 138. But for Defendant's wrongful and negligent breach of duties owed to  
5 Plaintiff and the Nationwide Class, the Private Information of Plaintiff and the Class  
6 would not have been compromised.

7  
8 139. Said differently, if Defendant had properly prevented a "technical  
9 security configuration," then the Data Breach would not have occurred, and  
10 Plaintiff's and Class Members' Private Information would have been appropriately  
11 safeguarded.

12  
13 140. Plaintiff and Class Members suffered an injury when their Private  
14 Information was accessed by unknown third parties.

15  
16 141. There is a close causal connection between Defendant's failure to  
17 implement security measures to protect the Private Information of Plaintiff and the  
18 Class and the harm, and the substantial risk of imminent harm, suffered by Plaintiff  
19 and the Nationwide Class.

20  
21 142. The Private Information of Plaintiff and Class Members was lost and  
22 accessed as the proximate result of Defendant's failure to exercise reasonable care  
23 in safeguarding such Private Information by adopting, implementing, and  
24 maintaining appropriate security measures.

25  
26 143. As a direct and proximate result of Defendant's breaches of its  
27  
28

1 fiduciary duties, Plaintiff and Class Members have suffered and will suffer injury,  
2 including but not limited to: (i) actual identity theft; (ii) the compromise,  
3 publication, and/or theft of their Private Information; (iii) out-of-pocket expenses  
4 associated with the prevention, detection, and recovery from identity theft and/or  
5 unauthorized use of their Private Information; (iv) lost opportunity costs associated  
6 with effort expended and the loss of productivity addressing and attempting to  
7 mitigate the actual and future consequences of the Data Breach, including but not  
8 limited to efforts spent researching how to prevent, detect, contest, and recover  
9 from identity theft; (v) the continued risk to their Private Information, which  
10 remains in Defendant's possession and is subject to further unauthorized  
11 disclosures so long as Defendant fails to undertake appropriate and adequate  
12 measures to protect the Private Information in their continued possession; (vi)  
13 future costs in terms of time, effort, and money that will be expended as result of  
14 the Data Breach for the remainder of the lives of Plaintiff and Class Members; and  
15 (vii) the diminished value of Defendant's services they received.

16  
17  
18  
19  
20  
21  
22 144. As a direct and proximate result of Defendant's negligence, Plaintiff and  
23 the Class have suffered and will continue to suffer other forms of injury and/or harm,  
24 including, but not limited to, anxiety, emotional distress, loss of privacy, and other  
25 economic and non-economic losses.

26  
27  
28 145. Additionally, as a direct and proximate result of Defendant's

1 negligence Plaintiff and the Class have suffered and will suffer the continued risks  
2 of exposure of their Private Information, which remains in Defendant's possession  
3 and is subject to further unauthorized disclosures so long as Defendant fails to  
4 undertake appropriate and adequate measures to protect the Private Information in  
5 its continued possession.  
6

7  
8 146. As a direct and proximate result of Defendant's negligence, Plaintiff  
9 and the Class are entitled to recover actual, consequential, and nominal damages.  
10

11 **COUNT II**  
12 **UNJUST ENRICHMENT**  
13 **(On behalf of Plaintiff and the Putative Nationwide Rule 23 Class)**

14 147. Plaintiff and the Class repeat and re-allege each and every allegation in  
15 the Complaint as if fully set forth herein.  
16

17 148. Plaintiff and Class Members conferred a monetary benefit on  
18 Defendant, by providing Defendant with their valuable Private Information.  
19

20 149. Defendant enriched itself by saving the costs they reasonably should  
21 have expended on data security measures to secure Plaintiff's and Class Members'  
22 Private Information.  
23

24 150. Instead of providing a reasonable level of security that would have  
25 prevented the Data Breach, Defendant instead calculated to avoid its data security  
26 obligations at the expense of Plaintiff and Class Members by utilizing cheaper,  
27  
28

1 ineffective security measures. Plaintiff and Class Members, on the other hand,  
2 suffered as a direct and proximate result of Defendant's failure to provide the  
3 requisite security.  
4

5 151. Under the principles of equity and good conscience, Defendant should  
6 not be permitted to retain the monetary value of the benefit belonging to Plaintiff  
7 and Class Members, because Defendant failed to implement appropriate data  
8 management and security measures that are mandated by industry standards.  
9

10 152. Defendant acquired the monetary benefit and Private Information  
11 through inequitable means in that they failed to disclose the inadequate security  
12 practices previously alleged.  
13  
14

15 153. If Plaintiff and Class Members knew that Defendant had not secured  
16 their Private Information, they would not have agreed to provide their Private  
17 Information to Defendant.  
18

19 154. Plaintiff and Class Members have no adequate remedy at law.  
20

21 155. As a direct and proximate result of Defendant's breaches of its duties,  
22 Plaintiff and Class Members have suffered and will suffer injury, including but not  
23 limited to: (i) actual identity theft; (ii) the compromise, publication, and/or theft of  
24 their Private Information; (iii) out-of-pocket expenses associated with the  
25 prevention, detection, and recovery from identity theft and/or unauthorized use of  
26 their Private Information; (iv) lost opportunity costs associated with effort  
27  
28

1 expended and the loss of productivity addressing and attempting to mitigate the  
2 actual and future consequences of the Data Breach, including but not limited to  
3 efforts spent researching how to prevent, detect, contest, and recover from identity  
4 theft; (v) the continued risk to their Private Information, which remains in  
5 Defendant's possession and is subject to further unauthorized disclosures so long  
6 as Defendant fails to undertake appropriate and adequate measures to protect the  
7 Private Information in their continued possession; (vi) future costs in terms of time,  
8 effort, and money that will be expended as result of the Data Breach for the  
9 remainder of the lives of Plaintiff and Class Members; and (vii) the diminished  
10 value of Defendant's services they received.

15 156. As a direct and proximate result of Defendant's conduct, Plaintiff and  
16 Class Members have suffered and will continue to suffer other forms of injury and/or  
17 harm.

19 157. Defendant should be compelled to disgorge into a common fund or  
20 constructive trust, for the benefit of Plaintiff and Class Members, proceeds that they  
21 unjustly received from them.

23 **COUNT III**  
24 **DECLARATORY AND INJUNCTIVE RELIEF**

25 158. Plaintiff and the Class repeat and re-allege each and every allegation in  
26 the Complaint as if fully set forth herein.  
27

1           159. Plaintiff pursues this claim under the Federal Declaratory Judgment  
2 Act, 28 U.S.C. § 2201.

3  
4           160. Under the Declaratory Judgment Act, 28 U.S.C. §§ 2201, *et seq.*, this  
5 Court is authorized to enter a judgment declaring the rights and legal relations of the  
6 parties and granting further necessary relief. Furthermore, the Court has broad  
7 authority to restrain acts, such as here, that are tortious and violate the terms of the  
8 federal statutes described in this Complaint.  
9

10  
11           161. An actual controversy has arisen in the wake of the Data Breach  
12 regarding Defendant's present and prospective common law and other duties to  
13 reasonably safeguard Plaintiff's and Class Members' Private Information, and  
14 whether Defendant is currently maintaining data security measures adequate to  
15 protect Plaintiff and Class Members from future data breaches that compromise their  
16 Private Information. Plaintiff and the Class remain at imminent risk that further  
17 compromises of their Private Information will occur in the future.  
18

19  
20           162. The Court should also issue prospective injunctive relief requiring  
21 Defendant to employ adequate security practices consistent with law and industry  
22 standards to protect employee and patient Private Information.  
23

24  
25           163. Defendant still possesses the Private Information of Plaintiff and the  
26 Class.  
27

1           164. To Plaintiffs' knowledge, Defendant has made no announcement that it  
2 has changed its data storage or retention practices relating to the Private Information.  
3

4           165. If an injunction is not issued, Plaintiffs and the Class will suffer  
5 irreparable injury and lack an adequate legal remedy in the event of another data  
6 breach at Houser LLP. The risk of another such breach is real, immediate, and  
7 substantial.  
8

9           166. As described above, actual harm has arisen in the wake of the Data  
10 Breach regarding Defendant's duties of care to provide security measures to  
11 Plaintiffs and Class Members. Further, Plaintiff and Class members are at risk of  
12 additional or further harm due to the exposure of their Private Information and  
13 Defendant's failure to address the security failings that led to such exposure.  
14

15           167. There is no reason to believe that Defendant's employee training and  
16 security measures are any more adequate now than they were before the breach to  
17 meet Defendant's legal duties.  
18

19           168. The hardship to Plaintiff and Class Members if an injunction does not  
20 issue exceeds the hardship to Defendant if an injunction is issued. Among other  
21 things, if another data breach occurs at Spear Wilderman, Plaintiff and Class  
22 Members will likely continue to be subjected to fraud, identify theft, and other harms  
23 described herein. On the other hand, the cost to Defendant of complying with an  
24  
25  
26  
27  
28

1 injunction by employing reasonable prospective data security measures is relatively  
2 minimal, and Defendant has a pre-existing legal obligation to employ such measures.  
3

4 169. Issuance of the requested injunction will not disserve the public interest.  
5 To the contrary, such an injunction would benefit the public by preventing another  
6 data breach at Spear Wilderman, thus eliminating the additional injuries that would  
7 result to Plaintiff and Class.  
8

9 170. Plaintiff therefore, seeks a declaration (1) that Defendant's existing data  
10 security measures do not comply with its duties of care to provide adequate data  
11 security, and (2) that to comply with its duties of care, Defendant must implement  
12 and maintain reasonable security measures, including, but not limited to, the  
13 following:  
14  
15

- 16 a. Ordering that Defendant engage internal security personnel to conduct  
17 testing, including audits on Defendant's systems, on a periodic basis,  
18 and ordering Defendant to promptly correct any problems or issues  
19 detected by such third-party security auditors;
- 20 b. Ordering that Defendant engage third-party security auditors and  
21 internal personnel to run automated security monitoring;
- 22 c. Ordering that Defendant audit, test, and train its security personnel and  
23 employees regarding any new or modified data security policies and  
24 procedures;
- 25 d. Ordering that Defendant purge, delete, and destroy, in a reasonably  
26 secure manner, any Private Information not necessary for its provision  
27 of services;
- 28 e. Ordering that Defendant conduct regular database scanning and  
security checks; and  
f. Ordering that Defendant routinely and continually conduct internal  
training and education to inform internal security personnel and  
employees how to safely share and maintain highly sensitive personal

1 information, including but not limited to, client personally identifiable  
2 information.

3 **PRAYER FOR RELIEF**

4 **WHEREFORE**, Plaintiff, on behalf of himself and Class Members, requests  
5 judgment against Defendant and that the Court grant the following:  
6

- 7 A. For an Order certifying the Class, and appointing Plaintiff and her  
8 Counsel to represent the Class;  
9
- 10 B. For equitable relief enjoining Defendant from engaging in the wrongful  
11 conduct complained of herein pertaining to the misuse and/or  
12 disclosure of the Private Information of Plaintiff and Class Members,  
13 and from refusing to issue prompt, complete, any accurate disclosures  
14 to Plaintiff and Class Members;  
15
- 16 C. For injunctive relief requested by Plaintiff, including, but not limited  
17 to, injunctive and other equitable relief as is necessary to protect the  
18 interests of Plaintiff and Class Members, including but not limited to  
19 an order:  
20
- 21 i. prohibiting Defendant from engaging in the wrongful and unlawful  
22 acts described herein;  
23
- 24 ii. requiring Defendant to protect, including through encryption, all  
25 data collected through the course of their business in accordance  
26  
27  
28

1 with all applicable regulations, industry standards, and federal, state  
2 or local laws;

3  
4 iii. requiring Defendant to delete, destroy, and purge the personal  
5 identifying information of Plaintiff and Class Members unless  
6 Defendant can provide to the Court reasonable justification for the  
7 retention and use of such information when weighed against the  
8 privacy interests of Plaintiff and Class Members;

9  
10  
11 iv. requiring Defendant to implement and maintain a comprehensive  
12 Information Security Program designed to protect the  
13 confidentiality and integrity of the Private Information of Plaintiff  
14 and Class Members;

15  
16 v. prohibiting Defendant from maintaining the Private Information of  
17 Plaintiff and Class Members on a cloud-based database;

18  
19 vi. requiring Defendant to engage independent third-party security  
20 auditors/penetration testers as well as internal security personnel to  
21 conduct testing, including simulated attacks, penetration tests, and  
22 audits on Defendant's systems on a periodic basis, and ordering  
23 Defendant to promptly correct any problems or issues detected by  
24 such third-party security auditors;

25  
26  
27 vii. requiring Defendant to engage independent third-party security  
28

auditors and internal personnel to run automated security monitoring;

viii. requiring Defendant to audit, test, and train their security personnel regarding any new or modified procedures;

ix. requiring Defendant to segment data by, among other things, creating firewalls and access controls so that if one area of Defendant's network is compromised, hackers cannot gain access to other portions of Defendant's systems;

x. requiring Defendant to conduct regular database scanning and securing checks;

xi. requiring Defendant to establish an information security training program that includes at least annual information security training for all employees, with additional training to be provided as appropriate based upon the employees' respective responsibilities with handling personal identifying information, as well as protecting the personal identifying information of Plaintiff and Class Members;

xii. requiring Defendant to routinely and continually conduct internal training and education, and on an annual basis to inform internal security personnel how to identify and contain a breach when it

- 1 occurs and what to do in response to a breach;
- 2 xiii. requiring Defendant to implement a system of tests to assess its
- 3 respective employees' knowledge of the education programs
- 4 discussed in the preceding subparagraphs, as well as randomly and
- 5 periodically testing employees compliance with Defendant's
- 6 policies, programs, and systems for protecting personal identifying
- 7 information;
- 8
- 9
- 10
- 11 xiv. requiring Defendant to implement, maintain, regularly review, and
- 12 revise as necessary a threat management program designed to
- 13 appropriately monitor Defendant's information networks for threats,
- 14 both internal and external, and assess whether monitoring tools are
- 15 appropriately configured, tested, and updated;
- 16
- 17
- 18 xv. requiring Defendant to meaningfully educate all Class Members
- 19 about the threats that they face as a result of the loss of their
- 20 confidential personal identifying information to third parties, as well
- 21 as the steps affected individuals must take to protect themselves;
- 22
- 23 xvi. requiring Defendant to implement logging and monitoring programs
- 24 sufficient to track traffic to and from Defendant's servers; and for a
- 25 period of 10 years, appointing a qualified and independent third
- 26 party assessor to conduct a SOC 2 Type 2 attestation on an annual
- 27
- 28

1 basis to evaluate Defendant's compliance with the terms of the  
2 Court's final judgment, to provide such report to the Court and to  
3 counsel for the class, and to report any deficiencies with compliance  
4 of the Court's final judgment;  
5

6 D. For an award of damages, including, but not limited to, actual,  
7 consequential, and nominal damages, as allowed by law in an amount  
8 to be determined;  
9

10 E. For an award of attorneys' fees, costs, and litigation expenses, as  
11 allowed by law;  
12

13 F. For prejudgment interest on all amounts awarded; and  
14

15 G. Such other and further relief as this Court may deem just and proper.  
16

17 **DEMAND FOR JURY TRIAL**

18 Plaintiff hereby demands that this matter be tried before a jury.

19 Date: March 5, 2024

20 Respectfully Submitted,

21 /s/ Joseph M. Lyon

22 Joseph M. Lyon (CA Bar # 351117)

23 **THE LYON FIRM**

24 2754 Erie Ave.

25 Cincinnati, OH 45208

26 Phone: (513) 381-2333

27 Fax: (513) 766-9011

28 *jlyon@thelyonfirm.com*

*Counsel for Plaintiff and Putative Class*

1  
2  
3  
4  
5  
6  
7  
8  
9  
10  
11  
12  
13  
14  
15  
16  
17  
18  
19  
20  
21  
22  
23  
24  
25  
26  
27  
28